Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of Parts 0, 1, 2, 15 and 18 of the	)	ET Docket No. 15-170
Commission's Rules regarding Authorization	)	
of Radio Frequency Equipment	)	
	)	
Request for Allowance of Optional Electronic	)	RM-11673
Labeling for Wireless Devices	)	

COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Sarah J. Morris
Senior Policy Counsel
Open Technology Institute | New America
1899 L Street NW, Suite 400
Washington, DC 20036

October 9, 2015

Introduction

Federal Communications Chairman Tom Wheeler has described unlicensed spectrum as "the sandbox where great innovations were born and now thrive."[1] He is right. However, it is not only the spectrum itself that has fostered innovation; an open and accessible transmission platform *combined* with devices and hardware that afford flexibility for tinkering and development comprise the overall ecosystem that has facilitated an explosion of new networks, tools, and systems.

If unlicensed spectrum is the sandbox of innovation, then open source software, particularly when used in conjunction with radio-enabled hardware, has served as the shovel and bucket. In the past decade, there has been a Cambrian explosion of wireless technologies, and there is a dynamic community of individuals leveraging platforms like OpenWrt to build and deploy wireless technology for myriad educational and practical purposes all around the world. From students starting out with Raspberry Pi devices to seasoned engineers, the ability to modify and deploy networked technology using open source software has permitted countless innovations in the wireless space. Using independent firmware allows software researchers and home users to adjust and improve network performance, increase security, and fix bugs in off-the-shelf router devices. Similarly, the OpenWrt platform also lies at the core of innovative mesh and community networks, and there have even been FCC-supported projects that utilize the OpenWrt platform to measure broadband performance,[2] as well as projects supported by other

[1] *See* Statement of Chairman Wheeler, *Amendment of the Commission's Rule with Regard to Commercial Operations in the 3550-3650 MHz Band, Report and Order and Second Further Notice of Proposed Rulemaking*, GN Docket No. 12-354 (rel. Apr. 17, 2015).

[2] *See* Federal Communications Commission, "2014 Measuring Broadband America, Technical Appendix" (rel. 2014), *available at* https://data.fcc.gov/download/measuring-broadband-america/2014/Technical-Appendix-fixed-2014.pdf.

branches of the government.[3]

However, even sandboxes require rules to ensure they remain a space in which all can play. Spectrum is a finite – and sometimes finicky – resource, which is why the Commission constantly endeavors to open bands for unlicensed use while simultaneously implementing appropriate rules to prevent harmful interference to licensed operations. There are various ways in which the Commission can protect against harmful interference, though the Commission notes in its proposed rulemaking that its "equipment authorization program is one of the primary means that the Commission uses to ensure that RF devices operating in the United States do not cause harmful interference and otherwise comply with our rules."[4]

While New America's Open Technology Institute (OTI) appreciates the role that equipment authorization can play in certain instances, we urge the Commission to exercise caution in adopting any changes to that process that would threaten innovation in the wireless space and curtail development of community broadband initiatives. The proposed new requirements could drive the proliferation of unnecessarily restrictive cryptographic measures that block access to software on a wide range of RF-enabled devices. Such expanded control measures would prevent local communities from repurposing off-the-shelf equipment for broadband deployment. By preventing individuals, startups, and non-commercial organizations from altering devices in entirely lawful ways that do not create the risk of harmful interference, such controls would also threaten more broadly to limit the innovation that has been the hallmark of the unlicensed bands.

[3] For example, OTI's Commotion Wireless Project received initial funding from the State Department. *See* "Commotion's Funding Sources," Commotion Wireless, *available at* https://commotionwireless.net/about/funding/.

[4] *In the Matter of Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules regarding Authorization of Radiofrequency Equipment; Request for the Allowance of Optional Electronic Labeling for Wireless Devices,* ET Docket No. 15-170, RM-11673, *Notice of Proposed Rulemaking*, FCC 15-170 (rel. Jul. 21, 2015) ("NPRM"), at ¶ 2.

I. The Commission should be wary of heightened certification requirements that would encourage device manufacturers to place locks on their devices in order to comply with those regulations.

The Commission notes that its certification and authorization process provides an extra "check" against the various spectrum management rules already in play.[5] Said another way, the Commission has enacted a spectrum regime in which it assigns certain spectrum bands to particular parties, leaving others available for unlicensed use. Devices certified to operate on any band are subject to certain rules of the road, including limits on transmission power and out of band emissions. The certification and authorization rules, in turn, provide an additional means by which the Commission ensures that manufacturers are making devices that play by the rules. It is important to note, however, that this additional oversight of device manufacturers can have significant downstream effects on the users who rely on those devices.

In the NPRM, the Commission "propose[s] to modify the SDR-related requirements in Part 2 of [its] rules based in part on the current Commission practices regarding software configuration control."[6] Importantly, the Commission notes that "[o]ur proposed rules would require that *all* manufacturers of devices that have software-based control of RF parameters must provide specific information about the software capabilities of their devices,"[7] and explains that an applicant for certification must "explicitly describe the RF device's capabilities for software configuration and upgradeability in the modulation types, or other modes of operation for which the device is designed to operate, including modes not enabled in the device as initially

[5] *See* infra at p. 2.

[6] NPRM at ¶ 46. The Commission further specifies that the proposal would require "an applicant for certification [to] explicitly describe the RF device's capabilities for software configuration and upgradeability in the modulation types, or other modes of operation for which the device is designed to operate, including modes not enabled in the device as initially marketed."

[7] NPRM at ¶ 46 (emphasis in original).

marketed."[8]

By placing this heightened certification onus on device manufacturers, where the manufacturers must anticipate the world of potential uses and users of products and certify that they cannot be operated in unauthorized bands or at unauthorized power levels, the Commission risks creating a scenario where, to guarantee compliance, the manufacturers have the incentive to implement restrictive software-based solutions that preclude the kind of tinkering and innovating that generates enormous public interest benefits.

It may well be the case that the Commission's proposed updated certification requirements could be met by manufacturers who certify simply that the chipsets used in their devices are region-locked at the baseband level. But it may also be the case that some manufacturers, because they are particularly risk-averse or because they lack the necessary knowledge or confidence to rely on statements regarding chipset-level protections built in by others, determine that the easiest way to meet the Commission's certification requirements is simply to lock down all middleware. After all, making sure that end users are able to modify and tinker with their devices is unlikely to be a priority for the vast majority of device manufacturers.

II. In order to build community wireless networks over open wireless platforms, OTI and others rely on making limited but important modifications to certain devices.

OTI is particularly concerned that the new requirements would encourage manufacturers to put in place barriers that would prevent the modification or enhancement of an RF-enabled device's software elements, a process commonly referred to as "reflashing." This could block the installation of widely-used and legal firmware such as OpenWrt or DD-WRT, device operating systems that serve as the foundation for many open source community networking projects. The impact and utility of such small community networks is demonstrated by their role in enhancing

[8] NPRM at ¶ 46.

community resilience and self-reliance during times of emergency or natural disaster, when conventional communications networks go offline. Many of the features necessary to construct such community networks using low-cost devices can only be found in innovative open-source firmwares.

For example, Commotion, a longstanding project at OTI funded initially by a U.S. State Department grant, is a wireless mesh networking platform that combines open source firmware with off-the-shelf hardware in order to empower communities to build their own communications infrastructure. The Commotion firmware contains a Linux-based operating system that is able to make use of only those radio interfaces exposed by the hardware. In fact, such open-source firmwares are often less able to make use of features such as DFS bands than proprietary firmwares, due to a lack of open implementations. However, if mechanisms like cryptographic signing of updates are recommended to manufacturers as a way to avoid unanticipated uses of certain bands, then such benign community projects might be locked out of the platforms on which they operate, despite their inability to infringe on those bands in the first place.

In another example, a community wireless network in Red Hook allowed community members to quickly reestablish connectivity in the wake of Superstorm Sandy, ensuring that residents of that neighborhood were able to communicate and quickly identify available resources such as food and water. In the days following the storm, up to 300 people per day were accessing the network to communicate with loved ones, understand what was happening in the city, and seek recovery assistance.[9] The network itself may never have been constructed if onerous certification requirements had foreclosed the space for the development of community

[9] *See* "Case Study: Red Hook Initiative WiFi and Tidepools," New America's Open Technology Institute (Feb. 2013), *available at* https://commotionwireless.net/files/rhiwifi_tidepools_casestudy.pdf.

wireless networks.

III. OTI urges the Commission to take a much more targeted approach of regulating RF devices that more carefully balances threats to innovation against threats of interference, utilizing an empirical understanding of the relative risks and costs.

OTI strongly urges the Commission to consider a different, less sweeping approach to enforcing rules that protect against harmful interference, and to carefully examine the likelihood of violations of band or power restrictions. Specifically, the Commission should focus its attention more squarely on the hardware layer of the devices, while explicitly encouraging openness at the firmware and software layers. However, before making any determinations about the need for additional protections, the Commission should undertake a thorough review of the potential interference harms that are likely to result as compared to the threat of harms to innovation that additional protections might create. Finally, the Commission should strongly consider whether ex post enforcement actions are the more appropriate avenue for mitigating interference, rather than ex ante limitations on the devices themselves.

Hardware vs. Firmware

Manufacturers of the types of carrier-grade RF hardware that are the most likely source of infringing interference have very effectively put region-locking protections into their hardware as part of the radio baseband, which third-party tools and firmware cannot easily modify. Many manufacturers have put region-locking protections in place for several years,[10] and these provide an extremely effective tool for keeping hardware from unduly interfering with other radio bands without further locking down devices against consumer software modifications. These existing protections, combined with import restrictions of international hardware, should be sufficient strategies for defending against the kinds of interference threats

[10] *See* Federal Communications Commission, *In the Matter of Ubiquiti Networks, Inc.* DA 13-295, *Order* (rel. Mar. 15, 2013), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-13-295A1.pdf.

that have existed in the past.

To defend against future threats, such as those that might be presented by interfering with database lookups (such as those mandated for “whitespace” devices), a trend towards clear, secure, and open interfaces for such lookups would benefit the users of both open source and proprietary software platforms on their RF devices. Even a proprietary protocol or interface may be tampered with, but mandating good engineering practices through well-defined software interfaces benefits proprietary projects as well as open source ones.

Need for Additional Evaluation

Before implementing any changes to its rules, the Commission should evaluate thoroughly the potential and likelihood for interference harms under its existing rules, and consider the full scope of harms to innovation in which the proposed changes to the rules may result. OTI expects that the record in this proceeding will be replete with examples of potential harms to innovation, and the Commission should take seriously those threats.

While interference can lead to substantial harms given the wide range of devices operating over wireless spectrum, the Commission’s NPRM does not suggest that harms of a significant magnitude are frequent. Weighing the potentially very low risk of significant interference harms against a high risk of far-reaching harms to wireless and open source innovation suggests the need to move forward with restraint in extensively modifying its current regulatory regime.

Enforcement vs. Rules

To the extent that the threats to innovation outweigh the risks of harmful interference, the Commission still has a mechanism through which it can address interference. Ex ante enforcement may allow the Commission to both mitigate the more egregious interference risks, without using additional prior restrictions that would hamstring innovation, and tie the hands of developers, researchers innovators, or other users of RF-Enabled devices.

Conclusion

OTI appreciates the need for the Commission to balance a diverse range of interests in this proceeding. However, the duty to preserve innovation in the wireless space is paramount. The Commission should refrain from modifying its rules in any way that would curtail the creation of new and innovative networked technologies, or harm the development of community broadband initiatives. In particular, the Commission should consider other less heavy-handed solutions that based on careful, detailed assessment of all potential harms.

Respectfully submitted,

/s/ Sarah Morris

Sarah J. Morris, Senior Policy Counsel
Laura M. Moy, Senior Policy Counsel
Josh King, Lead Technologist
Emily Hong, Program Associate
Michael Calabrese, Director, Wireless Future Program

Open Technology Institute | New America
1899 L Street NW, Suite 400
Washington, DC 20036